UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/913,595	10/22/2001	Manabu Sasamoto	501.40474X00	3782

20457 7590 02/08/2005

ANTONELLI, TERRY, STOUT & KRAUS, LLP
1300 NORTH SEVENTEENTH STREET
SUITE 1800
ARLINGTON, VA 22209-9889

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 02/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/913,595	**Applicant(s)** SASAMOTO ET AL.
	Examiner Matthew T Henning	**Art Unit** 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 August 2001*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-46* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 December 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *8/16/2001*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

This action is in response to the communication filed on 8/16/2001.

DETAILED ACTION

1. Claims 1-46 have been examined.

Title

2. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

Priority

3. This application is a 371 of PCT/JP99/00929 02/26/1999

4. The application has been filed under Title 35 U.S.C §371, claiming priority to PCT/JP99/00929, filed February 26, 1999.

5. The effective filing date for the subject matter defined in the pending claims in this application is 02/26/1999.

Information Disclosure Statement

6. The information disclosure statement (IDS) submitted on 8/26/2001 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statement.

Drawings

7. The drawings filed on 12/26/2001 are acceptable for examination proceedings.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claim 22 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

10. Claim 22 recites the limitation "said key information that has been updated" in line 4. There is insufficient antecedent basis for this limitation in the claim.

11. Claim 29 recites the limitation “witching” in line 10, which should read “switching”.

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> *(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

13. Claims 1-6, 19-25, and 39-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blatter et al. (US Patent Number 5,754,651) hereinafter referred to as Blatter, and further in view of Kulinets (US Patent Number 6,005,940).

14. Regarding claim 1, Blatter disclosed a digital signal recorder for recording a digital signal on a recording medium (See Blatter Abstract), comprising: key information generation means for generating at least one item of key information (encryption code) (See Blatter Col. 9 Lines 47-

50); key generation means which receive said key information and generate a key (See Blatter Col. 9 Lines 50-53); an encryption circuit which receives said key and said digital signal and encrypts said digital signal with said key and outputs the resulting encrypted digital signal (See Blatter Col. 5 Paragraph 2 wherein it was inherent that because the packets were encrypted using DES and decrypted with the generated key, and further because DES is a symmetric key encryption standard, the packets must have been encrypted with the generated key; and a recording circuit which records at least one of said items of key information, together with said encrypted digital signal, in prescribed area on said recording medium (See Blatter Col. 9 Lines 47-53 and Fig. 3 wherein the code was recorded in the CAT section along with the program), but Blatter failed to disclose how the key was generated from the encryption code, or that the key was generated by performing a prescribed arithmetic operation on the encryption code.

Kulinets teaches a method for generating an encryption key from key information (DK_A, and i) by performing block dependant arithmetic operations on the key information, in order to allow for encrypted storage (See Kulinets Fig. 8, Abstract, and Col. 6 Line 27 – Col. 7 Line 32).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Kulinets in the packet encrypting of Blatter by using the formula shown in Fig. 8 of Kulinets to generate the encryption key of Blatter by applying the encryption code and packet number of Blatter to DK_A and i of Kulinets respectively. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide a method for securely generating symmetric keys at both the encrypting and decrypting systems.

15. Regarding claim 2, the combination of Blatter and Kulinets disclosed that the digital signal has a packet format of a prescribed length (See Blatter Col. 12 Line 66 – Col. 13 Line 16).

16. Regarding claim 3, the combination of Blatter and Kulinets disclosed that the key information generation means have a function for updating at least one item of said key information at a prescribed time interval (See Kulinets Col. 6 Lines 49-52); and said recording circuit has a function for recording information capable of identifying timing wherewith said key information generation means update said key information, in prescribed area on said recording medium (See Blatter Col. 5 Paragraph 4).

17. Regarding claim 4, the combination of Blatter and Kulinets disclosed that the said digital signal has a packet format of a prescribed length (See Blatter Col. 13 Paragraph 1 wherein it was disclosed that the packet format was the MPEG standard, and therefore the packet must have been of the prescribed length of the MPEG standard); and said recording circuit has a function for adding information capable of identifying timing wherewith said key information generation means update said key information to packets of said digital signal and recording on said recording medium (See Blatter Col. 5 Paragraph 4 – Col. 6 Paragraph 2).

18. Regarding claim 5, the combination of Blatter and Kulinets disclosed that said encryption circuit further has a function capable of selecting between a function for encrypting and outputting said digital signal and a function for outputting said digital signal as is without encryption (See Blatter Col. 9 Lines 40-50); said recording circuit has a function for recording, in prescribed area on said recording medium, encryption flag information indicating whether or not said digital signal is encrypted, and when not encrypted, not recording said key information (See Blatter Col. 9 Lines 40-50 and Col. 4 Paragraph 4).

19. Regarding claim 6, the combination of Blatter and Kulinets disclosed that said digital signal has a packet format of a prescribed length (See rejection of claim 2 above); and said recording circuit has a function for adding encryption flag information indicating whether or not said digital signal is encrypted, to packets of said digital signal, and recording on said recording medium (See Col. 4 Paragraph 4).

20. Regarding claim 19, Blatter and Kulinets disclosed a digital signal reproducer for reproducing a digital signal recorded on a recording medium, comprising: a reproducing circuit which reproduces at least one item of key information recorded in prescribed area on said recording medium, and said digital signal (See Blatter Col. 9 Lines 50-53); key generation means which receive said key information and perform a prescribed arithmetic operation thereon to generate a key (See Blatter Col. 9 Lines 50-53 and rejection of claim 1 above); and a decryption circuit which receives said key and said reproduced digital signal and decrypts said digital signal with said key (See Blatter Col. 9 Lines 50-53 and Fig. 1 Element 50).

21. Regarding claim 20 see rejection of claim 2 above.

22. Regarding claim 21, Blatter and Kim disclosed generating the packet number and using it for generating the key (See rejection of claim 1 above).

23. Regarding claim 22, see the rejection of claim 3 above, wherein the decryption key was inherently updated in the same manner as the encryption key in order for the program to have been decrypted, and further because it was inherent that the key was switched to the updated key at the proper time (See Kulinets Col. 6 Lines 48-51 wherein the key is updated for each frame).

24. Regarding claim 23, see the rejection of claim 4 above, and see Kulinets Col. 6 Lines 48-51 wherein it was inherent that the frame number was reproduced).

25. Regarding claim 24, see the rejection of claim 5 above, wherein it was inherent that if the flag indicated that that the content was not encrypted, that the content would not be decrypted, and if it was encrypted that it would be decrypted (See Col. 4 Paragraph 4).

26. Regarding claim 25, see the rejection of claim 6 above, and further see Col. 4 Paragraph 4).

27. Regarding claim 39, see the rejection of claim 1 above and Blatter Fig. 3, and Col.2 Paragraph 3.

28. Regarding claim 40, see the rejection of claim 2 above.

29. Regarding claim 41, see the rejection of claim 3 above.

30. Regarding claim 42, see the rejection of claim 4 above.

31. Regarding claim 43, see the rejection of claim 5 above.

32. Regarding claim 44, see the rejection of claims 1 and 3 above wherein the encryption codes and packet numbers constitute the keys because they are the keys for creating the encryption keys.

33. Regarding claim 45, see the rejection of claims 19 and 44 above.

34. Regarding claim 46, see the rejection of claims 39 and 44 above.

35. Claims 7-17, and 26-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Blatter and Kulinets as applied to claim 1 above, and further in view of Kim (US Patent Number 6,466,733).

36. Regarding claim 7, the combination of Blatter and Kulinets disclosed a digital signal recorder in which a digital signal of a packet format of a prescribed length is input comprising: key information generation means for generating at least one item of key information; key

generation means which receive said key information and perform a prescribed arithmetic operation to generate a key; an encryption circuit which receives said key and said digital signal, encrypts said digital signal with said key and outputs the resulting encrypted digital signal; and a recording circuit which records at least one of said items of key information, together with said encrypted digital signal in prescribed area on said recording medium (See rejection of claims 1-2 above), but failed to disclose dividing the signal into other prescribed lengths; a synchronization signal, recording information signal, auxiliary information signal, and first error correction code are added thereto to define a block format; one track is formed by a prescribed number of blocks thus made; a second error correction code is added in units of n tracks (where n is an integer 1 or greater); said second error correction code is also divided and said first error correction code is added thereto to constitute a block format; and said tracks are recorded on said recording medium. However, the combination of Blatter and Kulinets did disclose the packet format being MPEG format.

Kim teaches a method for recording a digital transport stream by creating tracks from MPEG packets and providing three error correction codes to track (See Kim Figs. 2, 3, and 5 and Col. 6 Paragraphs 4-7 and Col. 7 Paragraphs 3-4),

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Kim in the recorder of Blatter and Kulinets by storing the encrypted packets in the ECC block format of Kim. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the stored programs against errors.

37. Regarding claim 8, see Blatter Col. 9 Lines 47-50, wherein the codes were stored in a conditional access table for each packet, which constitutes as an auxiliary storage area.

38. Regarding claim 9, see the rejection of claim 3 above.

39. Regarding claim 10, Kim disclosed that timing information was included in the stored block data (see Kim Col. 5 Paragraph 6).

40. Regarding claim 11, Kim disclosed that timing information was stored in an auxiliary section (See Kim Col. 6 Paragraph 4 and Col. 7 Paragraph 3).

41. Regarding claim 12, Kim disclosed adding timing information to the blocks identifying the timing of the packets (See Kim Col. 2 Lines 54-57)

42. Regarding claim 13, see Kulinets Col. 6 Lines 49-52 wherein the key was updated for each packet, and therefore for each track as well. This was because each track contained at least one packet.

43. Regarding claim 14, see Blatter Col. 9 Lines 40-50, wherein it was disclosed that the encryption code was generated only if the program was to be stored in encrypted form.

44. Regarding claim 15, see Blatter Col. 10 Lines 32-34, wherein the CAT is stored in the Condensed Program Specific Information, and Col. 9 Lines 47-50, wherein the CAT stored the encryption code.

45. Regarding claim 16, see Blatter Claims 20-21 wherein the CPSI is stored in the auxiliary area.

46. Regarding claim 17, see the rejection of claim 6 above.

47. Regarding claim 26, see the rejection of claims 7 and 19 above.

48. Regarding claim 27, see the rejection of claim 21 above.

49. Regarding claim 28, see Kulinets Col. 6 Lines 48-52, and the rejection of claim 8 above.

50. Regarding claim 29, see Kulinets Col. 6 Lines 48-52, and the rejection of claim 9 above wherein it was inherent that the key was switched to the updated key with each frame in order to have decrypted the program.

51. Regarding claim 30, see the rejection of claim 10 above, and further Blatter Col. 5 Paragraph 4).

52. Regarding claim 31, see the rejection of claim 11 above and further Blatter Col. 5 Paragraph 4).

53. Regarding claim 32, see the rejection of claim 12 above, and further Blatter Col. 5 Paragraph 4).

54. Regarding claim 33, see the rejection of claim 13 above.

55. Regarding claim 34, see the rejection of claim 14 above and claim 24 above.

56. Regarding claim 35, see the rejection of claim 15 above.

57. Regarding claim 36, see the rejection of claim 16 above.

58. Regarding claim 37, see the rejection of claim 17 above.

59. Claims 18 and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Blatter, Kulinets, and Kim as applied to claims 14 and 34 above, and further in view of Yuval et al. (US Patent Number 5,586,186), hereinafter referred to as Yuval.

The combination of Blatter, Kulinets, and Kim disclosed determining if a program would be stored in encrypted form or not (See Blatter Col. 9 Lines 40-50), but failed to disclose encrypting or not based on each track.

Yuval teaches that in order to secure information in an efficient manner, only some of the tracks should be encrypted (See Yuval Col. 6 Lines 12-23).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Yuval in the encryption system of Blatter, Kulinets, and Kim by only encrypting every nth track. This would have been obvious because the ordinary person skilled in the art would have been motivated to improve the efficiency of both the encoding and decoding of the programs.

Conclusion

60. Claims 1-46 have been rejected.

61. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Okada et al. (US Patent Number 4,635,113) disclosed a system for descrambling television signals including sending a key id with the signal.

b. Ibaraki et al. (US Patent Number 5,546,461) disclosed a system for recording a video signal in which a key is generated from a seed and the key is used to encrypt the signal, and the seed is set to the descrambler in order to generate the correct descramble key.

c. Yanagihara (US Patent Number 5,835,668) disclosed a system for recording a scrambled signal.

d. Ishibashi (US Patent Number 6,021,199) disclosed a system for encrypting an MPEG-2 stream, or recording.

62. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew Henning
Assistant Examiner
Art Unit 2131

Andrew Caldwell
ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER